PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 12/14

A1

(11) International Publication Number: **WO 95/16238**

(43) International Publication Date: 15 June 1995 (15.06.95)

(21) International Application Number: PCT/US94/13898

(22) International Filing Date: 5 December 1994 (05.12.94)

(30) Priority Data:
08/161,854 6 December 1993 (06.12.93) US

(71) Applicant: TELEQUIP CORPORATION [US/US]; 18 Clinton Drive, Hollis, NH 03049 (US).

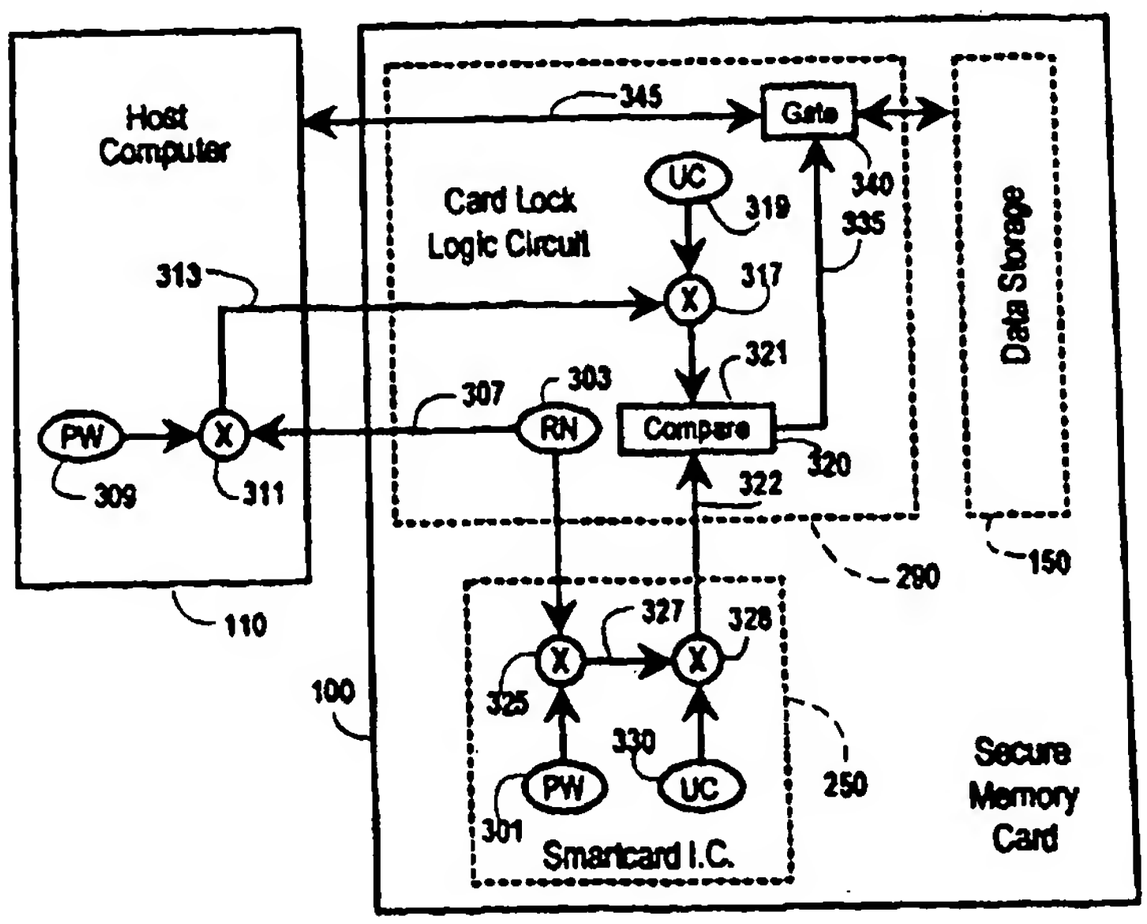
(72) Inventors: JONES, Michael, F.; 7 Foxglove Court, Nashua, NH 03062 (US). ZACHAI, Arthur; 22 Ross Road, Swampscott, MA 01907 (US).

(74) Agents: CALL, Charles, G. et al.; Allegretti & Witcoff, Ltd., Ten South Wacker Drive, Chicago, IL 60606 (US).

(81) Designated States: AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MN, MW, NL, NO, NZ, PL, PT, RO, RU, SD, SE, SI, SK, TJ, TT, UA, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), ARIPO patent (KE, MW, SD, SZ).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SECURE COMPUTER MEMORY CARD



(57) Abstract

A detachable PCMCIA memory card (100) incorporating a smartcard integrated circuit (250) for storing a password value and logic circuitry for preventing access to information stored on the memory card (100) unless the user of the host computer (110) to which the memory card (100) is connected can supply a password matching the stored password. The smartcard integrated circuit (250) may also be used to store public and private key values used to encrypt and decrypt data stored on the card (100) or elsewhere on the host computer (110) or exchanged with a remote computer (120).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**GB**	United Kingdom	**MR**	Mauritania
AU	Australia	**GE**	Georgia	**MW**	Malawi
BB	Barbados	**GN**	Guinea	**NE**	Niger
BE	Belgium	**GR**	Greece	**NL**	Netherlands
BF	Burkina Faso	**HU**	Hungary	**NO**	Norway
BG	Bulgaria	**IE**	Ireland	**NZ**	New Zealand
BJ	Benin	**IT**	Italy	**PL**	Poland
BR	Brazil	**JP**	Japan	**PT**	Portugal
BY	Belarus	**KE**	Kenya	**RO**	Romania
CA	Canada	**KG**	Kyrgyzstan	**RU**	Russian Federation
CF	Central African Republic	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CG	Congo			**SE**	Sweden
CH	Switzerland	**KR**	Republic of Korea	**SI**	Slovenia
CI	Côte d'Ivoire	**KZ**	Kazakhstan	**SK**	Slovakia
CM	Cameroon	**LI**	Liechtenstein	**SN**	Senegal
CN	China	**LK**	Sri Lanka	**TD**	Chad
CS	Czechoslovakia	**LU**	Luxembourg	**TG**	Togo
CZ	Czech Republic	**LV**	Latvia	**TJ**	Tajikistan
DE	Germany	**MC**	Monaco	**TT**	Trinidad and Tobago
DK	Denmark	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**US**	United States of America
FI	Finland	**ML**	Mali	**UZ**	Uzbekistan
FR	France	**MN**	Mongolia	**VN**	Viet Nam
GA	Gabon				

SECURE COMPUTER MEMORY CARD

FIELD OF THE INVENTION

This invention relates generally to methods and apparatus for storing, processing and communicating private data.

BACKGROUND OF THE INVENTION

Computers are widely used to store and process information which is considered private. For most businesses, the confidentiality of computer data is maintained using the practice followed for conventional business data: restricting access to office space where sensitive records are kept, whether those records take the form of documents kept in file cabinets or machine-readable data stored in an computer.

As the capabilities and usefulness of laptop and notebook computers have increased, functions formerly performed within the security of the office have moved to the field. Sales personnel and executives often travel with computers loaded with confidential data on pricing, customers, and strategic planning. Although available encryption and decryption programs can be used to protect such data when it is not in use, these programs are often inconvenient to use or provide poor security as a result of inadequate key management.

Encryption methods typically rely on "secret keys" known only to authorized users of the protected data. In the widely used Data Encryption Standard ("DES") developed and promulgated by the National Bureau of Standards, data is encyphered in 64-bit blocks using a single 56-bit key, as described in NBS FIPS PUB 46, "Data Encryption Standard," National Bureau of Standards (1977). Encryption techniques using two keys, one for encypting the data and a different key for decryption, are called "public key" systems because the encryption key can be made public so that anyone can use the public key to encrypt sensitive data, but only a recipient with the secret key can decrypt it. One widely used and highly effective public key algorithm known as the "RSA" system is described in Rivest et al. U.S. Patent 4,405,829.

The security of both single-key and public-key encryption systems depends on user's ability to keep the key or keys secret. Although both the DES and RSA encryption algorithms themselves can be depended upon to provide

adequate security, neither system can safeguard data if the keys can be learned. The management of the keys themselves accordingly presents the most difficult component of good data security system.

SUMMARY OF THE INVENTION

It is an object of the invention to securely store private information in a compact, easily transportable storage device which may be detached from the computer with which it is used.

It is still another object of the invention to protect such electronically stored data against unauthorized access when the detachable storage device is lost or stolen.

It is a further object of the present invention to provide a secure data storage device which may, at the option of the user, selectively limit access to all or part of the stored data using one or more passwords.

It is a related object of the invention to securely store access passwords, encryption or decryption keys, or digital signatures, in a tamper-proof substorage unit interconnected with a data access mechanism which are integral parts of a detachable computer memory card.

In a principle aspect, the present invention takes the form of a removable memory card, preferably implemented in conformity with the PCMCIA interface standard, which provides the host computer to which it is connected with additional high-speed storage, the memory card consisting of a data storage unit, storage-access locking circuitry, and a tamper-proof key information substorage unit. In accordance with the invention, the locking circuitry is adapted to prevent access to the data stored on the memory card unless the would-be user first presents identifying information which is validated by the locking circuitry with reference to one or more key values stored in the key information substorage unit.

The removable memory card contemplated by the present invention allows data stored on the card to be made immediately available to the connected host computer upon proper presentation of a password known only to an authorized user. Once the password has been validated, the stored data may then be made available to the host processor in decrypted form.

In accordance with the invention, the key information substorage unit advantageously takes the form of a "smartcard" integrated circuit capable of storing secret key values which may be used to provide password-protected access

to the data stored on the memory card, or optionally to provide secure storage for the encryption or decryption keys, or digital signatures, needed to allow the host computer to access and/or operate a secure information storage or telecommunications system. In accordance with the invention, access to data, passwords, digital signatures, or other key values stored on the memory card is limited to those who (1) have physical possession of the memory card and (2) knowledge of the memory card access password stored in the card's secure substorage unit.

The smartcard integrated circuit advantageously stores such passwords, public key and secret key values, and/or digital signatures in an Electrically Erasable Programmable Read Only Memory (EEPROM), and further includes its own microprocessor containing a stored program to allow reading and writing of the EEPROM through a serial I/O interface. The stored program within the smartcard IC allows an access password to be programmed into the EEPROM from an external source via the serial interface, but thereafter prevents that password value from being accessed. For enhanced security, the smartcard integrated circuit includes means for monitoring voltages and frequencies to detect abnormal conditions which may indicate an attempt to tamper with the key storage unit to gain unauthorized access to the stored secret key information.

These and other objects, features and advantages of the present invention will become more apparent by considering the following detailed description of a preferred embodiment of the invention, during which frequent reference will be made to the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 of the drawings is a block diagram of a secure memory card which embodies the principles of the invention, the memory card being shown interconnected with a host computer which is in turn connected to other computers by telecommunications links.

Figure 2 is a data flow diagram depicting a preferred mechanism for providing password protection for information stored within a memory card of type shown in Fig. 1.

Figure 3 is a data flow diagram illustrating the use of a secure data card as show in Fig. 1 to protect the privacy of information being sent between a host computer and a remote computer.

DESCRIPTION OF THE PREFERRED EMBODIMENT

HARDWARE

As illustrated in Fig. 1 of the drawings, the preferred embodiment of the invention takes the form of a personal computer memory card indicated generally at 100. The memory card 100 is interconnected with a host computer 110 by means of a hardware and software interface which conforms to the Personal Computer Memory Card International Association (PCMCIA) standard which has been widely accepted for use in laptop and notebook computers. PCMCIA cards are commonly used to provide additional high-speed memory capacity to the connected host computer, or to implement fax and data modems, network access devices, and hard-disk mass storage devices. Type 1 PCMCIA cards have a form factor typically used to provide additional memory for data and application programs, while the thicker Type 2 cards are used to add telecommunications features and Type 3 cards are used for high-capacity hard disk drives that store up to 100 megabytes of data.

The removable character of PCMCIA storage devices can provide better data security than storage built into the computer itself, because the card may be detached from the computer and placed in a secure area when not in use. However, the cards themselves remain subject to possible theft or misuse. The embodiment of the invention shown in Fig. 1 provides significant additional security for data and programs stored in a detachable memory card by incorporating an access-locking mechanism for preventing access to the stored data by those who are unable to present an authorizing password.

The secure memory card 100 contemplated by the invention is adapted to be connected via its PCMCIA interface to the host computer 110 which may in turn be connected to other computers by modem, or by a network, as illustrated by the connection of remote computer 120 via the telecommunications link 130 seen in Fig. 1.

The secure memory card 100 stores data in a common memory array 150, preferably implemented with non-volatile flash memory integrated circuits, enabling the common memory array to store 10 megabytes of data in an area small enough to be included on a credit-card sized Type I PCMCIA card. The data is stored in random access locations specified by address values supplied via the PCMCIA's standard 26-bit address bus terminals 161. The address terminals 161 provide address signals to an input address bus buffer circuit 163 which

drives an internal address bus 165. Data transfers between the common memory array 150 and the host computer 110 are accomplished via the interface data terminals 171, a data bus buffer 173, an internal data bus 175, a internal encyption/decryption unit 177, a gate 178 and an internal data bus 179. Control signals are exchanged between the common memory array 150 and the host computer via the PCMCIA interface control terminals 181 and an internal control bus 185.

The address terminals 161, data terminals 171 and control terminals 181 seen in Fig. 1 are a simplified representation of the 68 pin PCMCIA standard interface which includes provision for 26 parallel address conductors (A0-A25), 16 parallel data conductors (D0-D15), and a remaining set of power and control conductors including power and ground connections and a collection of memory control signal connections (enable, select, wait, write, detect, etc.). The PCMCIA standard achieves interchangeability of cards of different functions by establishing standards for the physical card (dimensions and mechanical tolerances for the card and connectors), the card interface (pinout and signal definitions), and card software (which specifies the organization of data on the card and the record formats and protocols by which configuration information and data is exchanged with the host computer). Complete information which defines the PCMCIA standard is published by and available from the Personal Computer Memory Card International Association, 1030G East Duane Avenue, Sunnyvale, CA 94086. The present embodiment of invention conforms to the PC Card Standard Specification, Release 2.01, published in November, 1992.

To implement the PCMCIA interface standard, the secure memory card includes a non-volatile attribute memory 190 which stores information enabling the host computer to automatically identify the particular PCMCIA card as soon as the card and host are connected, and to automatically establish the appropriate hardware/software interface using suitable driver software which executes on the host computer 110.

The attribute memory 190 shares the internal address bus 165, data bus 175 and control bus 185 with the common memory array 150. An address decoder 195 monitors the address bus 165 and provides selection signals to the attribute memory 190 via a attribute memory enable line 197 when addresses within the address space of attribute memory 190 appear on address bus 165 concurrently with the activation of the Attribute Memory Select signal terminal -REG (not separately shown in Fig. 1) in the PCMCIA connector interface.

Similarly, the address decoder 195 selects the common memory array 150 whenever the address on address bus 165 is within the address space of array 150 by energizing an common memory enable line 210 which supplies an enable signal to the gate 178 in the data pathway to the common memory array 150.

Gate 178 prevents the common memory array 150 from exchanging data with the host 150 via data bus 179 unless an authorization signal is supplied to the gate 200 via a control line 219 from a card lock logic circuit 220. The card lock logic circuit 210 is connected to address decoder 195 via the lock enable line 221, permitting card logic 220 to identify addresses which designate memory locations in the common memory array 150 to which access may be denied under appropriate circumstances. The card lock logic circuit 220 is connected to the internal data bus 175 which provides a pathway for downloading memory access control commands from the host computer 110.

A smartcard input/output enable line 198 transmits an enable signal from the address decoder 195 to a Universal Asynchronous Receiver Transmitter (UART) 230 when information is to be transferred between the host computer 110 and a smartcard integrated circuit 250. The UART 230 is connected to the internal data bus 175 and operates to translate data received in bit-parallel form from databus 175 into bit serial form for transfer to the smartcard I.C. via its serial port 255.

The smartcard I.C. includes its own processor 260 and non-volatile EEPROM memory circuits 257 which operate as a secret key information substorage system. The processor 260 within the smartcard I.C. 250 is programmed to store secret key codes within the EEPROM 257, but to thereafter prohibit the stored secret keys from being accessed by any external interrogation. The smartcard I.C. may be implemented with a number of available devices, including the ST16F48 CMSO MCU-based Safeguarded Smartcard IC, with 8k EEPROM, available for SGS-Thomson Microelectronics, a member of the SGS-Thomson ST16XYZ family of devices, as specified in the SGS-Thomson Data Book (April, 1993). The ST16F48 includes an 8-bit processor, 288 bytes of RAM scratchpad storage, an 8k byte EEPROM data memory which forms the secure substorage unit, and a 16k byte program storage read-only memory for storing processing routines, including routines for processing and validating key values supplied to and read from the smartcard I.C. via the UART 230.

Data transfers and operations, both within the memory card 100 and between the card 100 and the host computer 110, are controlled by the card lock

logic circuit 220. When the lock circuit enable line 221 is activated in response to the detection of an access control command address value by address decoder 195, the card lock logic circuit 220 responds to commands and data supplied to the internal data bus 175 from the host computer 110 via the data conductors 171 and the data bus buffers 173. The card lock logic circuit 220, the UART 230 and the smartcard I.C. 260 operate under the control of a common timing signal provided by an on-card clock generator circuit seen at 290 in Fig. 1.

The address space provided by the common memory array 150 is preferably partitioned into independently accessed regions. Each partition is specified in a Card Information Structure or "CIS" (to be described) which is stored in the attribute memory 190, and preferably corresponds to the memory space provided by one or more integrated circuits making up the array 150 such that a particular partition may be selected by the address decoder 195 which activates particular chip enable lines with the common memory enable output 210.

The access password itself is stored in the EEPROM 257 within the smartcard I.C. 250, the password storage operation being accomplished within the memory card 100 whenever a card lock logic activation address is supplied via address terminals 161 and the address buffer 163 to the address decoder 195 which in turn activates the card logic enable line 221. A password loading command applied via the data interface terminals 171 from the host computer is recognized by card lock logic 220 which channels the subsequent data sequence (the password itself) via the UART 230 and the serial port 255 of the smartcard I.C. 250 for storage at a predetermined location in the EEPROM 257.

Once a password has been stored for a particular partition, the card lock logic circuit 220 has exclusive control over access to that partition. Any attempt to access that partition (as detected by the address decoder 195) will be rejected, notifying the device driver software that a valid password must be provided. The driver software then prompts the user with a request for a valid password which, when entered, is sent via the data buffer 173 for validation. The card lock logic 220 routes the offered password to the smartcard I.C. with a request that it be compared with the password stored in the EEPROM 257. If the passwords match, the smartcard I.C. so notifies the card lock logic 220 which in turn notifies the device driver software executing in the host that the partition has been successfully unlocked. Thereafter, when addresses within the unlocked partition are detected by the address decoder 195, the card lock logic will

activate the gate 178 to permit data transfers between that partition and the data terminals 171.

To provide additional security, the data transferred over the 16-bit data bus between the data bus buffer 173 and the gate 178 is processed by the encryption-decryption unit 177 which preferrably emplements a symmetrical key algorithm, such as DES, based on a key value which stored in and fetched from the EEPROM 275 in the smartcard I.C. 250. The unit 250 encrypts data from the data bus buffer 173 prior to storing the data in the common memory array 150, and decrypts the data back into its original form when it is retrieved from the common memory array 150. This additional encryption mechanism protects data stored in the common memory array even if that data is successfully read from the flash memory chips making up the array 150. As discussed in more detail later, the secure key storage mechanism provided by the memory card may also be used to protect sensitive data being manipulated by mechanisms external to the memory card 100.

All of the operative circuitry making up the memory card 100, with the exception of the attribute memory 190, the common memory array 150, and the smartcard I.C. 250, is preferrably implemented by means of a single, monolithic application specific integrated circuit (ASIC) as indicated within the dashed line rectangle 290 in Fig. 1. By integrating this circuitry in a monolithic integrated circuit, security against invasive attempts to ascertain built-in unlock codes (to be discussed) or to bypass or disable security functions, is substantially improved.

SOFTWARE

As previously noted, the attribute memory 190 stores information which specifies the nature of the memory card 100 and the format used for the information stored on the card. The attribute memory 190 holds a Card Information Structure ("CIS") which is organized in a "Metaformat" defined in Section 5 of the PCMCIA PC Card Standard, Release 2.01, for handling numerous different data recording formats. The CIS is organized as hierarchy of layers and takes the form of a chain (linked-list) of data blocks called "tuples" which begin at address 0 of the attribute memory 190.

The PCMCIA standard also establishes standards for the operation of host processor operating system software which can be used to simplify the design of specific device drivers which provide access to the memory card. The standard "Socket Services" and "Card Services" card interface software, when implemented

on a given host computer, provides a Card Services interface with "Client Device Drivers," significantly simplifying the design of device drivers by providing much of the functionality required for communicaton with socketed PCMCIA cards. For host computers which are not provided with standard PCMCIA Card Services and Socket Services functions, the device driver directly interrogates the CIS structures in the attribute memory using standard link-list processing techniques, and provide direct software support for the bulk memory functions which would otherwise be supported by the PCMCIA Card Services interface.

Whether utilizing available Card Services routines or directly addressing and manipulating the memory card hardware interface, the device drive itself may be specified in the DOS CONFIG.SYS file and loaded when the host processor is initialized, or may take the form of an independently loadable TSR program. The discussion which follows describes the operation of a Client Device Driver adapted to operate in conjunction with PCMCIA standard Card Services functions and notification mechanisms.

The programming interface to the PCMCIA Card Services software is defined in Section 3 of the PCMCIA Standard (Release 2.01) which specifies a variety of services which are available to Client Device Drivers, as well as callback mechanisms for notifying Client Device Drivers of status changes. In addition to conventional memory operations provided by Bulk Memory Service functions, the Card Services software also provides Client Utility functions which allow client device drivers to access and manipulate the CIS stored in the memory card's attribute memory 190. Card management routines, either forming a part of the Client Device Driver or part of a special purpose application program for configuring the memory card according to the users needs, are executed on the host computer. These card management routines in turn utilize the functions provided by the PCMCIA Card Services software to implement the following two special operations which not required for conventional PCMCIA memory cards:

PARTITION LOCK. This operation accepts two parameters from the user: (1) a password value, typically taking the form of ASCIIZ (null-terminated string) of keyboarded characters entered by a user in response to a prompt, and (2) a partition identifier which specifies a portion of the address space provided by the common memory array 150. At the same time, the fact that a given partition has been locked, together with the an identification of the EEPROM

memory location of the password (but not its value) are recorded in the CIS entry for that partition.

The memory card 100 is intitialized as a standard memory card before being first delivered to the end user, and provides one or more freely accessible storage partitions prior to receiving the first PARTITION LOCK command.

PARTITION UNLOCK. The storage of a password associated with a particular password has the effect of locking that password against subsequent attempts to use the data or programs stored within that partition without first supplying a valid password.

Whenever a PCMCIA card is newly inserted into the socket of a running host computer, the Client Device Driver is notified by the Card Services software (via its CARD_INSERTION callback function), so that it can process the card's CIS entries to identify each partition that may be password-protected. Similarly, when the host computer is first powered up and the Client Device Driver is initialized, the Client Device Driver calls Card Services functions to process the cards CIS entries to identify each partition that may be locked.

The device driver software then attempts to access each identified partition. If the partition is locked (as determined by the mechanism discussed above), the card lock logic 220 notifies the device driver of the locked condition, allowing the device driver to request a valid password from the user, either at the time the host computer is being initialized with an already socketed memory card, or at the time a memory card is first inserted into an already running host computer.

Other Operatons. To support encryption and decryption systems, systems employing digital signatures, and secure telecommunications access protocols, examples of which will be discussed below, the card lock logic unit 220 and UART 230 also provide the capability for storing additional passwords, key values, access codes and the like in the secure substorage system provided by the smartcard I.C. 250, or alternatively (but less securely) in the common memory array 150 or in the attribute memory 190.

PASSWORD AND KEY MANAGEMENT

A preferred mechanism for validating the user's password needed to unlock a particular memory partition is illustrated in Fig. 2 of the drawings. First, as previously described, the user who desires to protect information stored

on the card supplies a secret password which is written into the smartcard I.C. memory as indicated at 301. When an attempt is made to access data protected by the secret password 301, the ASIC 290 implementing the card lock logic unit 220 generates a random number 303 which is supplied to the host computer 110 as indicated at 307. The host computer 110 then prompts the user to enter a password at 309. The offered password 309 is combined with the random number 303 at 311 and the result is returned at 313 to the ASIC 290. The returned value is then combined at 317 with a fixed unlock code 319 (built into the ASIC 290) to produce a final value which is applied to a first input 321 of a comparator 320.

At the same time, the random number 303 which was sent to the host is also sent to the smartcard I.C. 250 whose processor 260 is programmed to combine the random number 303 at 325 with the previously stored secret password 301 to form a result value at 327. The result value 327 is combined at 328 with a copy 330 of the unlock code 319, and the resulting final value is applied to the second input 322 of the comparator 320. If the final value at input 321 which is created by the password offered by the user matches the final value at input 322 created by the password stored within the smartcard I.C. 250, the partition associated with the stored password will be unlocked by sending an activation signal 335 to a data flow gate 340 connected in the path of a data bus 345 connecting the host computer 350 and the memory card's common memory array 360.

It is important to observe that the data stored in a protected partition within the memory card 100 is available only to those who possess <u>both</u> the card and the password. Neither possession of the card without knowledge of the password, nor knowledge of the password without physical possession of the card, will be sufficient to obtain access to the data.

The combined requirement that the bearer of the card also know the password can be used to provide security for data stored or transmitted outside the memory card, as well as for data stored within the card, as illustrated by the examples depicted in Fig. 3 of the drawings.

As depicted in Fig. 3, a secure memory card 400 is connected to a host computer 410 and includes a smartcard integrated circuit 415 which provides a secure substorage system which stores a password 420, an access code 425, a private key value 430, and a public key value 435.

The password 420 is used to verify the identity of the bearer of the memory card, who is required to enter of a valid password 440 when prompted by the host computer as previously discussed in conjunction with Fig. 2. Unless a

valid password 440 is known to the bearer of the memory card 400, the additional codes and keys 425, 430 and 435 cannot be retrieved from the smartcard I.C. Requests for access to the a stored key is passed to the smartcard I.C. and processed by routines stored in the smartcard I.C. internal ROM program store, which denies any incoming request which is not accompanied by the submission af a valid password 440. However, if the bearer of the memory card 400 can provide a valid password 440 which matches the stored password 420, the following additional secure transactions are made possible between the host computer 410 and a remote computer 450.

First, the remote computer 450 may deny access to one or more of its capabilities unless a proper access code is transmitted from a would be remote station which establishes communications with the computer 450, typically via a dial-up telephone connection using modem transmission, or by a dedicated connection in a network or the like. By storing the needed access code in the a password-protected PCMCIA card, an improved mechanism is provided form establishing the authority of a remote caller to access designated functions in the remote computer. Preferably, the validity of the stored access code is established by a challenge-and-response exchange of the type illustrated in Fig. 2, in which the remote computer 450 transmits a challenge in the form of a random number which is combined with the stored access code 425 to form a response which is returned to the remote computer 450 for verification. In this way, the access code 425 is not transmitted and interception of either the challenge or response values by an intruder monitoring the exchange will not provide the intruder with the access code.

After the host computer 410 establishes its identity to the satisfaction of the remote computer 450 using the stored access code 425, the host computer then may request the transmission of encrypted data from the remote computer. To accomplish this, the two stations may use a two key encryption and decryption mechanism in which the remote computer 450 encrypts the data to be transmitted with a public key 455 and the host computer, using the private key value 430 stored in the smartcard I.C. 415, decrypts the received transmission to obtain the desired message text. Other computers in the network in possession of the public key 455 may also send secure transmissions to the host computer 410, but cannot decrypt such messages from others since only the possessor of the private key 430 is able to decrypt the transmissions.

Alternatively, the smartcard I.C. may store one or more public key values such as the public key 435 which enables the host processor to send secure transmissions to a selected remote receiving computer in possession of the corresponding private key 460. In the same way, single key encryption mechanisms such as DES, and systems requiring the identification of remote senders using digital signature techniques can be readily implemented using the password protected secure memory card as the mechanism for storing the needed key values.

The DES and RSA Encryption schemes, as well as numerous other systems for the secure information transmission and retention are described in detail in *Applied Cryptography: Protocols, Algorithms, and Source Code in C* by Bruce Scheier, John Wiley & Sons (1994), ISBN 0471597562. The use of the detachable, password protected secure memory card contemplated by the present invention provides additional security by providing an improved key management mechanisms which requires that a would-be user of such a system have both physical possession of the memory card (which holds the needed key values) and knowledge of the password which permits the key values to be accessed.

It is to be understood that the specific mechanisms and techniques which have been described are merely illustrative of on application of the principles of the invention. Numerous modifications may be made to the methods and apparatus described without departing from the true spirit and scope of the invention.

What is claimed is:

1. A secured personal computer memory card comprising, in combination,

a plurality of interface conductors adapted to mate with corresponding conductors in a personal computer connector socket, said interface conductors establishing data, address, control and power pathways between said card and said personal computer,

a non-volatile data storage memory connected to said data and address pathways,

an integrated circuit comprising, in combination, a substorage memory unit for storing secret data, and means for processing a password supplied from said personal computer in accordance with said secret data to generate an authorization signal when said password has a predetermined correct value while otherwise preventing access to said secret data by means external to said integrated circuit, and

memory access control means for preventing said personal computer from accessing data stored in said data storage memory via said data and address pathways in the absence of said authorization signal.

2. A secure personal computer memory card as set forth in claim 1 wherein said memory access control means includes means for selectively encrypting and decrypting data transferred over a data pathway connecting said interface terminals to said data storage memory.

3. A memory storage card comprising, in combination,

a plurality of electrical terminals adapted for connection to said host computer, said terminals including address teminals, data terminals and control terminals,

one or more integrated circuits forming a common memory array for storing data at storage locations specified by address values applied as binary signal values to said address terminals, said data being tranferred to and from said common memory array by connections to said host computer established by said data terminals,

a memory substorage unit comprising an integrated circuit consisting of a processor and a programmable memory device, and

a card lock logic unit comprising, in combination,

an address decoder for generating control signals in response to the detected presence of predetermined ones of said address signal values,

means responsive to a first one of said control signals for transferring a first password value supplied by said host computer via said data terminals to said memory substorage unit to place at least a portion of said common memory array in a locked state,

means responsive to a second one of said control signals for preventing the flow of data between said data terminals and said portion said common memory array when said portion is in said locked state,

means for evaluating a second password value available to said host computer to determine if said second password value bears a predetermined relationship to said said first password value, and

means for placing said portion of said commonn memory array in an unlocked state when said predetermined relationship is identified.

4. A memory storage card as set forth in claim 1 further comprising, in combination,

encryption means connected between said data terminals and said common memory array for enciphering data prior to storage in said common memory array in accordance with a key value stored in said memory substorage unit, and

decryption means connected between said common memory array and said data terminals for deciphering data retrieved from said common memory array in accordance with a key value stored in said memory substorage unit.

5. A memory storage card as set forth in claim 1 wherein said card lock logic unit takes the form of a monolithic integrated circuit.

6. A memory storage card as set forth in claim 1 further including gate means connected between said data terminals and said common memory array, said gate means being responsive to said address decoder for placing said portion in said locked state by preventing the flow of data to or from said memory array whenever said address decoder detects a request to transfer data to or from said portion of said memory array.

7. The method of protecting information against unauthorized access comprising, in combination, the steps of:

storing the data to be protected in the common memory array of a memory card,

providing said memory card with an integrated circuit for storing a password in a protected substorage memory,

storing an arbitrarily selected password in said protected substorage memory,

providing an electronic logic circuit on said memory card for comparing said arbitrary selected password stored in said substorage memory with a password submitted in support of a request to access said data, and

transfering requested data from said common memory array in response to said request only if the submitted password bears a predetermined matching relationship with said password stored in said protected substorage memory.

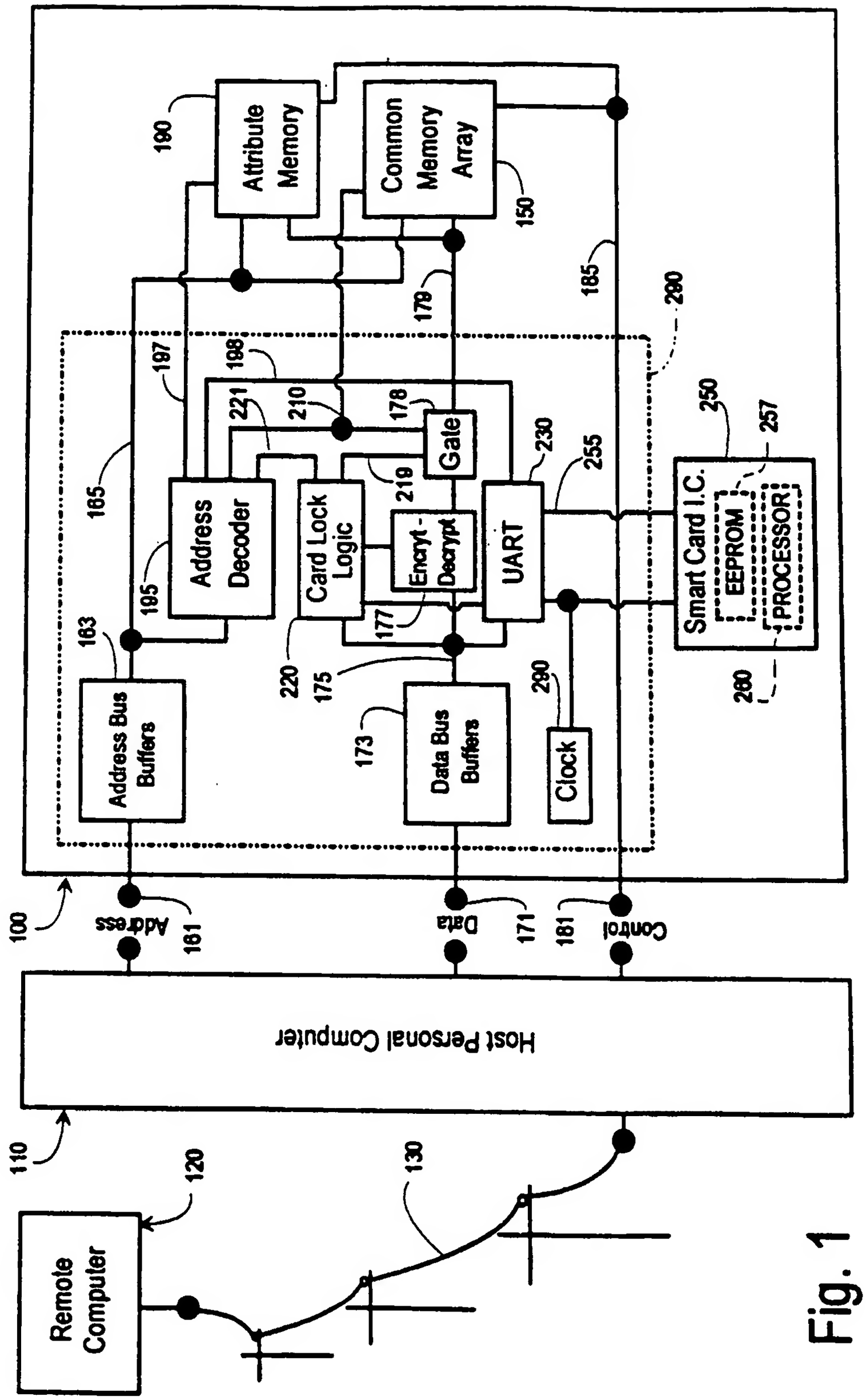

Attribute Memory
Common Memory Array
190
150
185
179
290
197
198
221
210
178
Gate
219
Address Decoder
Card Lock Logic
Encryt-Decrypt
UART
230
255
250
257
Smart Card I.C.
EEPROM
PROCESSOR
280
185
195
163
177
220
175
173
Address Bus Buffers
Data Bus Buffers
290
Clock
100
Address
181
Data
171
181
Control
Host Personal Computer
110
120
Remote Computer
130

Fig. 1

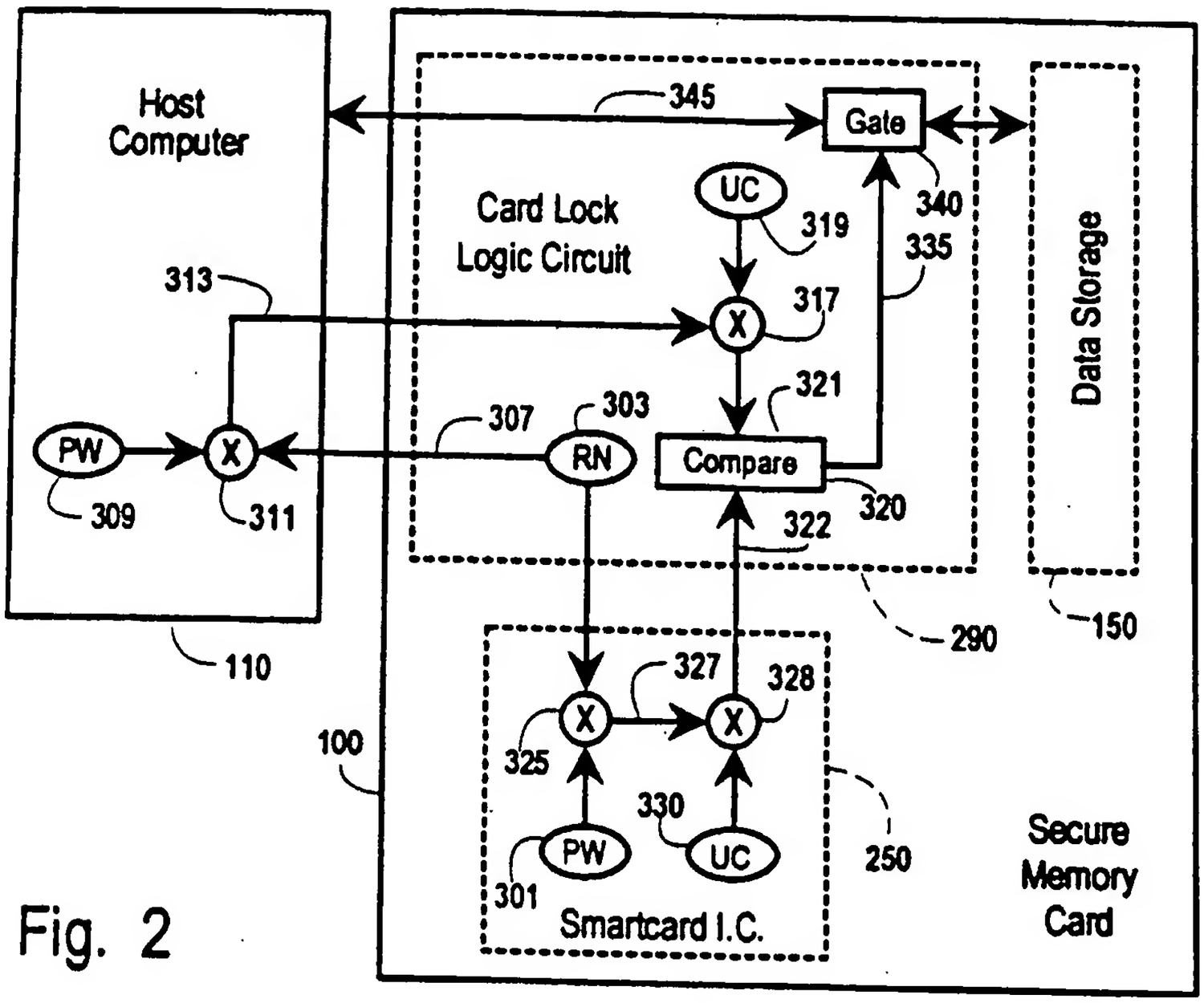

Host Computer
110
345
Gate
340
Card Lock Logic Circuit
UC
319
335
313
317
X
321
307
303
PW
X
RN
Compare
309
311
322
320
Data Storage
290
150
327
328
X
X
100
325
330
PW
UC
250
301
Smartcard I.C.
Secure Memory Card

Fig. 2

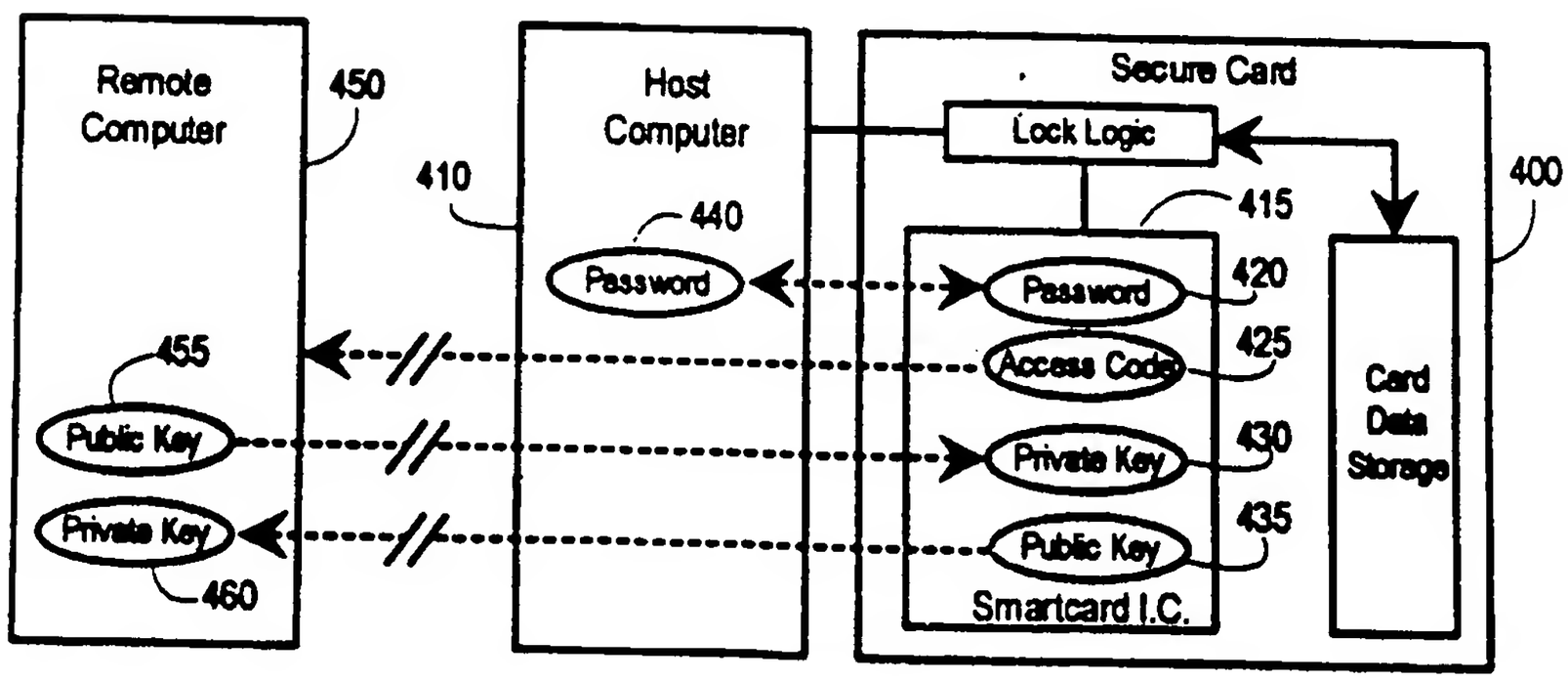

Remote Computer
450
Host Computer
410
Secure Card
Lock Logic
400
440
415
Password
420
Password
455
425
Access Code
Card Data Storage
Public Key
430
Private Key
Private Key
435
Public Key
460
Smartcard I.C.

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US94/13898

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G06F 12/14
US CL :395/425;380/23

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 395/425;380/23

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS, smartcard, security, authorization, password, memory lock, memory protection

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US, A, 5,068,894 (HOPPE) 26 November 1991, col. 1, line 38 to col. 4, line 53.	1-7
Y	US, A, 5,204,663 (LEE) 20 April 1993, col. 1, line 63 to col. 3, line 2.	1-7
X,P --- Y,P	US, A, 5,293,424 (HOLTEY ET AL) 08 March 1994, col. 2, line 42 to col. 4, line 15.	1, 3, 5-7 --- 2, 4
Y,P	US, A, 5,341,428 (SCHATZ) 23 August 1994, col. 2, lines 25-68.	1-7
Y,P	US, A, 5,347,580 (MOLVA ET AL) 13 September 1994, col. 5, line 20 to col. 6, line 52.	1-7

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be part of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
01 FEBRUARY 1995	20 APR 1995
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer REBA I. ELMORE Telephone No. (703) 305-3819

Form PCT/ISA/210 (second sheet)(July 1992)*